september 2018

**PRIVACY CHECKLIST VOOR DE OR**

Introductie AVG

Per 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze verordening somt de beginselen en uitgangspunten voor de verwerking van persoonsgegevens op en bevat de rechten die betrokkenen hebben met betrekking tot hun persoonsgegevens. De AVG moet ervoor zorgen dat organisaties op een zorgvuldige manier omgaan met persoonsgegevens van bijvoorbeeld werknemers, klanten, patiënten etc.

AVG en medezeggenschap

De AVG bestaat naast de WOR. De AVG noemt de OR niet als betrokken orgaan. De invoering van de AVG in organisaties is op zichzelf ook niet advies- of instemmingsplichting. Dat betekent niet dat de OR geen enkele positie heeft. Veel organisaties voeren veranderingen door als gevolg van de AVG. Bij het doorvoeren van die veranderingen beschikt de OR mogelijk over een advies- of instemmingsrecht. De OR moet bij de uitoefening van deze rechten ook privacyaspecten betrekken. Het is daarom van belang dat de OR op de hoogte is van de AVG. Deze checklist schetst op hoofdlijnen de kaders die op grond van de AVG gelden. Let op: niet alle onderwerpen die de AVG regelt, zijn in deze checklist uitputtend opgenomen.

Toepasselijkheid AVG

De AVG is van toepassing als sprake is van *verwerking* van *persoonsgegevens*.

*Persoonsgegevens*

Persoonsgegevens zijn “alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon”. Het gaat om informatie die gebruikt kan worden om een persoon te identificeren. Iemand is bijvoorbeeld identificeerbaar aan de hand van zijn naam, identificatienummer, locatiegegevens en (e-mail)adres, maar ook aan de hand van andere elementen die kenmerkend zijn voor zijn fysieke, psychologische, genetische, economische, culturele, of sociale identiteit, zoals geslacht, bankgegevens, religie of politieke voorkeur. Het maakt niet uit of de identificatie direct (door middel van een naam of een geboortedatum) of indirect plaats kan vinden (via een simpele koppeling van systemen, zoals kentekennummers en kadastergegevens). Let op: het gaat alleen om gegevens die zien op levende, natuurlijke personen. Gegevens van overleden natuurlijke personen en gegevens over rechtspersonen zijn geen persoonsgegevens in de zin van de AVG.

Voorbeelden van persoonsgegevens in een arbeidsrelatie zijn bijvoorbeeld de naam en contactgegevens van een werknemer, zijn geboortedatum, de hoogte van zijn salaris, de opleidingen die hij genoten heeft, maar ook informatie over zijn aanwezigheid en/of ziekteverzuim, of een foto op een badge of camerabeelden.

Het is van belang onderscheid te maken tussen ‘gewone’ persoonsgegevens en bijzondere persoonsgegevens, zoals gezondheidsgegevens, gegevens over godsdienst, gegevens over seksuele voorkeur, gegevens over politieke voorkeur, etc. Voor de verwerking van bijzondere persoonsgegevens geldt een strikter regime met aanvullende waarborgen.

*Verwerking*

Verwerking is “een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens”.

Kort gezegd wordt met verwerking gedoeld op vrijwel alle mogelijke handelingen met betrekking tot persoonsgegevens die men kan bedenken. Dit betekent dat de AVG al snel van toepassing is.

Rollen en bijbehorende verantwoordelijkheden

De AVG hanteert verschillende rollen voor partijen die betrokken zijn bij de verwerking van persoonsgegevens. De drie belangrijkste rollen zijn de onderstaande rollen.

- De *betrokkene* is degene over wie de persoonsgegevens gaan (in de arbeidsrelatie doorgaans de werknemer);
- De *verwerkingsverantwoordelijke* is degene die het doel en de middelen voor de verwerking vast stelt (in de arbeidsrelatie is dit doorgaans de werkgever);
- De *verwerker* is degene die ten behoeve van de verwerkingsverantwoordelijke gegevens verwerkt (in de arbeidsrelatie is dit bijvoorbeeld een externe salarisadministratiekantoor of een externe verzuimbegeleider).

Afhankelijk van welke rol een partij inneemt, volgen er rechten en plichten uit de AVG. Zo kunnen betrokkenen bepaalde rechten uitoefenen (zie hieronder) en moet de verwerkingsverantwoordelijke daaraan gehoor geven.

Ook in de relatie tussen de verwerkingsverantwoordelijke en de verwerker gelden specifieke plichten. De AVG bepaalt namelijk dat de verwerkingsverantwoordelijke en verwerker een overeenkomst moeten sluiten waarin een aantal essentialia over de verwerking worden vastgelegd. Deze overeenkomst noemt men ook wel de verwerkersovereenkomst.

Op grond van de AVG moeten in een verwerkersovereenkomst de volgende punten vastgelegd worden:

- Onderwerp en duur van de verwerking
- De aard en het doel van de verwerking
- Soort persoonsgegevens en categorieën van betrokkenen
- Rechten en verplichtingen verwerkingsverantwoordelijke
- Instructievereiste
- Waarborgen vertrouwelijkheid
- Genomen beveiligingsmaatregelen
- Inzet andere verwerkers
- Bijstandverlening bij vervulling verzoeken betrokkenen
- Bijstandverlening bij voldoen aan beveiligingseisen, meldplicht datalekken en gegevensbeschermingseffectbeoordeling
- Omgaan persoonsgegevens bij einde overeenkomst
- Mogelijk maken van audits

Uiteraard kunnen partijen in een verwerkersovereenkomst ook meer onderwerpen regelen. Denk aan afspraken over aansprakelijkheid, schade, het opleggen van een boete, informatieverplichtingen over en weer etc.

Basisbeginselen

De AVG bepaalt dat iedere verwerking van persoonsgegevens aan een aantal vereisten moet voldoen. Het gaat om de volgende zes beginselen.

- Rechtmatigheid, behoorlijkheid en transparantie: persoonsgegevens moeten worden verwerkt op een wijze die rechtmatig, behoorlijk en transparant is.
- Doelbinding: persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet worden verwerkt op een wijze die niet verenigbaar is met die doeleinden.

- Minimale gegevensverwerking: persoonsgegevens moeten toereikend zijn, maar wel ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor ze worden verwerkt.
- Juistheid: persoonsgegevens moeten juist zijn en waar nodig worden geactualiseerd en men moet het redelijke doen om persoonsgegevens die onjuist zijn te wissen of te rectificeren.
- Opslagbeperking: persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt om de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de verwerking noodzakelijk is (denk aan maatregelen als anonimiseren, pseudonimiseren of versleuteling).
- Integriteit en vertrouwelijkheid: men moet passende technische en/of organisatorische maatregelen ter beveiliging nemen en persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen (onbedoeld) verlies, vernietiging of beschadiging.

<u>Grondslagen</u>

Daarnaast moet er voor iedere verwerking een grondslag bestaan. Een verwerking is alleen rechtmatig en dus toegestaan als deze op een van de volgende zes grondslagen is gebaseerd.

- Toestemming: een verwerkingsverantwoordelijke kan persoonsgegevens verwerken op basis van de door de betrokkene verleende toestemming. Toestemming moet vrijelijk, specifiek, geïnformeerd en ondubbelzinnig gegeven worden. Let op: in een arbeidsrelatie moet men oppassen met het gebruik van toestemming als grondslag. Omdat er sprake is van een gezagsrelatie, is het sterk de vraag of de toestemming in vrijheid gegeven kan worden. Een andere grondslag verdient de voorkeur. De betrokkene heeft altijd het recht om de toestemming in te trekken. De grondslag vervalt dan.
- Uitvoering van een overeenkomst of nemen van precontractuele maatregelen. Hieronder kan ook vallen het uitvoeren van een arbeidsovereenkomst.
- Wettelijke verplichting: een verwerkingsverantwoordelijke kan persoonsgegevens verwerken als dit noodzakelijk is om een wettelijke verplichting na te komen die op hem rust.
- Vitaal belang: een verwerkingsverantwoordelijke kan persoonsgegevens verwerken als dit noodzakelijk is om de vitale belangen van een betrokkene of een andere natuurlijke persoon te beschermen.
- Taak van algemeen belang of openbaar gezag: een verwerkingsverantwoordelijke kan persoonsgegevens verwerken als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of een taak in het kader van de uitoefening van openbaar gezag.
- Belangenafweging: een verwerkingsverantwoordelijke kan persoonsgegevens verwerken als dat noodzakelijk is voor de behartiging van zijn eigen gerechtvaardigde belangen of de gerechtvaardigde belangen van een derde. Daarbij moet een belangenafweging worden gemaakt of dit gerechtvaardigde belang zwaarder weegt dat de (privacy)belangen, grondrechten en fundamentele vrijheden van de betrokkenen. Alleen als het gerechtvaardigde belang zwaarder weegt dan de belangen van de betrokkene, kan deze grondslag gebruikt worden.

<u>Rechten van betrokkenen</u>

De AVG kent betrokkenen (degenen over wie de persoonsgegevens gaan) de volgende individuele rechten toe:

- Recht op inzage (en kopie) van persoonsgegevens
- Recht op rectificatie van persoonsgegevens
- Recht op gegevenswissing (‘recht om vergeten te worden’)
- Recht op beperking van de verwerking van persoonsgegevens
- Recht op overdraagbaarheid van gegevens (‘recht van dataportabiliteit’)
- Recht van bezwaar
- Recht om niet onderworpen te worden aan geautomatiseerde individuele besluitvorming

Naast deze individuele rechten geldt een algemeen informatierecht. Een verwerkingsverantwoordelijke moet degenen over wie persoonsgegevens worden verzameld van bepaalde informatie voorzien. De AVG schrijft voor welke informatie de verwerkingsverantwoordelijke aan de betrokkene moet verstrekken. Vaak gebeurt dit door middel van een privacyverklaring.

Verwerkingsregister

Voor bepaalde organisaties geldt de verplichting om een verwerkingsregister bij te houden. Dit geldt in ieder geval voor organisaties met meer dan 250 personen in dienst of voor organisatie met minder dan 250 personen die aan bepaalde criteria voldoen.

Uiteraard mag een organisatie ook op vrijwillige basis een verwerkingsregister bijhouden. De AVG schrijft voor welke informatie het verwerkingsregister moet bevatten. Dit is ook afhankelijk van de rol die de organisatie inneemt (verwerkingsverantwoordelijke of verwerker).

Meldplicht datalekken

Een datalek doet zich voor wanneer er sprake is van "een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot verwerkte persoonsgegevens".

De meldplicht voor datalekken is opgenomen in de AVG. Dit betekent dat organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens en/of de betrokkene als er binnen hun organisatie sprake is van een (ernstig) datalek. Let op: niet elk datalek hoeft bij de Autoriteit Persoonsgegevens en/of de betrokkene gemeld te worden. Dit is afhankelijk van het type datalek en de mogelijke gevolgen. De organisatie moet in ieder geval een register bijhouden van alle datalekken die zich voordoen.

Functionaris voor de gegevensbescherming

De AVG introduceert de functionaris voor de gegevensbescherming. Dit is een onafhankelijk en deskundig persoon met als taak het informeren, adviseren en aanbevelingen doen over de omgang met persoonsgegevens en het analyseren en controleren van de wijze waarop persoonsgegevens verwerkt worden.

Een organisatie kan verplicht of onverplicht een functionaris voor gegevensbescherming aanstellen. De AVG geeft de criteria om te bepalen of een organisatie verplicht een functionaris moet aanstellen.

De AVG stelt een aantal eisen aan de functionaris voor de gegegevensbescherming, onder meer inzake zijn bereikbaarheid en deskundigheid. Ook onverplicht aangestelde functionarissen moeten aan alle wettelijke vereisten voldoen.

Let op: er bestaat enige discussie over de vraag of de aanstelling van de functionaris voor de gegevensbescherming instemmingsplichtig is. Inmiddels wordt veelal het standpunt ingenomen dat dit niet het geval is. Er is – in tegenstelling tot de preventiewerker – geen specifieke bepaling waarin de OR een instemmingsrecht toegekend krijgt.

OR en privacy

Zoals aangegeven heeft de OR geen specifieke rechten met betrekking tot de invoering van de AVG. Wel beschikt de OR over de rechten die voortvloeien uit de WOR. De twee meest in het oog springende WOR-rechten van de OR die verband houden met privacyaspecten, zijn de volgende.

- De OR heeft een instemmingsrecht ten aanzien van een regeling omtrent het verwerken van persoonsgegevens van de in de onderneming werkzame personen. Ook op deze verwerking van persoonsgegevens is de AVG van toepassing. De OR kan (moet) de regels vanuit de AVG dus meewegen in zijn oordeel of hij wel of niet instemming verleent.

- De OR heeft een instemmingsrecht ten aanzien van een regeling inzake een personeelscontrolesysteem (= voorzieningen die gericht zijn op of geschikt zijn voor waarnemingen van prestaties van de in de onderneming werkzame personen). Let op: het enkele feit dat een voorziening geschikt is om het personeel te controleren, is voldoende voor instemmingsplichtigheid. De voorziening hoeft dus niet per se ook bedoeld te zijn om personeel te controleren. Vaak leiden personeelscontrolesystemen tot verwerking van persoonsgegevens. Ook op deze verwerking van persoonsgegevens is de AVG van toepassing. De OR kan (moet) de regels vanuit de AVG dus meewegen in zijn oordeel of hij wel of niet instemming verleent.

Daarnaast kunnen privacyaspecten ook voor andere rechten van de OR van belang zijn. Zo kan verwerking van persoonsgegevens een rol spelen in het kader van adviesplichtige besluiten. Denk bijvoorbeeld aan een voorgenomen besluit tot fusie of overname waarbij persoonsgegevens van medewerkers gedeeld worden of overgaan of aan een voorgenomen besluit tot het invoeren van een belangrijke technologische voorziening die (mogelijk) persoonsgegevens verwerkt. Ook in die gevallen dient de OR waar nodig aan de AVG te toetsen.

Daarnaast is de ondernemer verplicht twee keer per jaar overleg te voeren met de OR over de algemene gang van zaken in de onderneming. Daarin moet hij mededeling doen van de te verwachten advies- of instemmingsplichtige besluiten. Mogelijk kunnen in deze vergadering ook besluiten in het kader van (de invoering van) de AVG naar voren komen.

De ondernemer is verplicht om de OR alle informatie te verstrekken die de OR redelijkerwijs nodig heeft voor de vervulling van zijn taak. Mogelijk heeft de OR voor een goede vervulling van zijn taak informatie over privacyaspecten nodig.

Tot slot kan de OR zelf privacyaspecten aan de orde stellen door middel van het initiatiefrecht. Onderstaande checklist biedt aanknopingspunten hiervoor. Zo kan de OR bijvoorbeeld nagaan of de verwerkingsverantwoordelijke een verwerkingsovereenkomst met eventuele verwerkers heeft afgesloten (en of deze aan de voorwaarden voldoet), of aan eventuele verplichtingen tot het hebben van een verwerkingsregister is voldaan en of er een adequate procedure voor het melden van datalekken bestaat, etc. Als de OR hier gebreken in constateert, kan hij de ondernemer daarop wijzen.

Uiteraard kan de OR op grond van de cao of in een ondernemingsovereenkomst over extra rechten met betrekking tot privacyaspecten beschikken.

<u>Gegevens verwerken als OR</u>
Ook de OR verwerkt in sommige gevallen persoonsgegevens, bijvoorbeeld in het kader van een instemmings- of adviesaanvraag of in het kader van OR-verkiezingen. De OR dient zich dan te houden aan de AVG. De OR valt als orgaan van de verwerkingsverantwoordelijke onder de paraplu van diens verantwoordelijkheid. Dat betekent dat de OR zelf niet aangesproken kan worden op een privacy schending: de eindverantwoordelijkheid ligt namelijk bij de verwerkingsverantwoordelijke. Dat betekent uiteraard niet dat de OR zich niet aan de regels hoeft te houden.

**AVG-CHECKLIST**

Op deze pagina zijn 18 vragen opgenomen die de OR (zichzelf of de ondernemer) kan stellen. Een deel van de vragen kan de OR meer in het algemeen stellen, een deel van de vragen is ook in het kader van een advies- of instemmingsaanvraag van belang.

1. Is sprake van persoonsgegevens?
2. Is sprake van verwerking?
3. Welke partij neemt welke rol in bij de verwerking van persoonsgegevens? Wie is de verwerkingsverantwoordelijke en zijn er verwerkers ingeschakeld? Indien er verwerkers ingeschakeld zijn: is er een verwerkingsovereenkomst gesloten die voldoet aan de wettelijke vereisten?
4. Welke grondslag geldt er voor de verwerking van persoonsgegevens en is voldaan aan de vereisten om van die grondslag gebruik te maken?
5. Wat is het doel van de verwerking van persoonsgegevens? Zijn alle verwerkingen in lijn met dit doel en worden de persoonsgegevens niet voor andere doeleinden gebruikt (doelbinding)?
6. Worden niet meer gegevens verwerkt dan noodzakelijk is om het doel te bereiken?
7. Zijn voldoende maatregelen genomen om te waarborgen dat de persoonsgegevens juist en nauwkeurig zijn?
8. Zijn voldoende passende beveiligingsmaatregelen genomen? Waar worden persoonsgegevens bijvoorbeeld opgeslagen en wie heeft er toegang tot de persoonsgegevens?
9. Moet er een verwerkingsregister bijgehouden worden en gebeurt dat ook?
10. Heeft de organisatie een procedure voor het melden van datalekken en wordt een datalekkenregister bijgehouden?
11. Moet er een functionaris voor gegevensbescherming worden aangesteld en is dat gebeurd?
12. Worden persoonsgegevens verstrekt aan personen of partijen buiten de organisatie? Zo ja, gebeurt dit conform de regels van de AVG?
13. Vindt gegevensverkeer naar landen buiten de Europese Unie plaats? Zo ja, zijn er aanvullende maatregelen genomen c.q. afspraken gemaakt zoals beschreven in de AVG?
14. Hoelang worden de persoonsgegevens bewaard? Is deze termijn niet langer dan noodzakelijk?
15. Worden bijzondere persoonsgegevens verwerkt en is voldaan aan de aanvullende regels die daarvoor gelden?
16. Worden betrokkenen (medewerkers) juist en volledig geïnformeerd over de verwerking van hun persoonsgegevens?
17. Zijn betrokkenen (medewerkers) op de hoogte van hun rechten en weten zij hoe zij hiervan gebruik kunnen maken?
18. Van welke rechten kan de OR gebruik maken? Is er bijvoorbeeld sprake van een voorziening die gericht is op of geschikt is voor het controleren van personeel, of van een regeling inzake het verwerken of het beschermen van persoonsgegevens?

Meer weten over de gevolgen van de AVG voor uw organisatie en de rol van de OR daarbij?
Neem contact op met mr. drs. Manouk Milbou of mr. drs. Els Huisman, advocaten bij De Voort Advocaten | Mediators, via m.milbou@devoort.nl en 013-4668884 of e.huisman@devoort.nl en 013-4668882.

Opgesteld op verzoek van SBCM